Computer search for curves with many points among certain quotient curves of the Fermat curves

Computer search for curves with many points among certain quotient curves of the Fermat curves

Motoko Qiu Kawakita

ABSTRACT

We make computer search among curves defined by $y^a = x^b(1-x^c)^d$ over $\mathbb{F}_{p^n}$ where p does not divide a and c, one of $\gcd(a, b+cd)$, $\gcd(a,d)$ and $\gcd(a,b)$ is 1. As the result we find new curves with many rational points, where we can update many entries of manypoints.org.

1. *Introduction*

Let p be a prime number and $n \in \mathbb{N}$ where $\mathbb{N} := \{1, 2, \ldots\}$. We set $\mathbb{F}_q$ as a finite field with $q = p^n$. By a curve we mean a smooth geometrically irreducible projective curve. Explicit curves with many rational points have many applications in coding theory, cryptography and quasi-random points; see [4], [8], [9]. Let $N_q(g)$ denote the maximum number of $\mathbb{F}_q$ rational points among the curves of genus g defined over $\mathbb{F}_q$. We have the Hasse–Weil bound

$$N_q(g) \leq q + 1 + 2g\sqrt{q}.$$

The curve is said to be maximal if it attains this bound. In 1983 Serre improved it as

$$N_q(g) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor,$$

which we call the Serre bound. Here $\lfloor\ \rfloor$ denotes the round down. Nowadays, van der Geer et al. collect the results of $N_q(g)$ as tables in [3]. However there are many lower bounds of the entries remaining empty, which means that we know no curve of that genus g with many rationl points over the finite field $\mathbb{F}_q$.

On the other hand, quotient curves of the Fermat curves have studied by Faddeev in [1], Koblitz and Rohrlich in [7]. Garcia et al. showed that many maximal curves can be constructed from quotient curves of the Hermitian curve in [2]. In addition we also have quotient curves of the Fermat curves attaining the Serre bound for some non square q in [6]. These observations motivate us to make computer search on quotient curves of the Fermat curves to find more curves with many rational points.

2. *Computer search*

In this section we explain about our computer search. First we determine the defining equations of curves to do search.

LEMMA. *Let k be a field of characteristic p. Let a, b, c, $d \in \mathbb{N}$ where p does not divide a and c, one of* $\gcd(a, b+cd)$, $\gcd(a,d)$ *and* $\gcd(a,b)$ *is* 1. *Then the polynomial* $Y^a - X^b(1-X^c)^d$ *is*

2000 *Mathematics Subject Classification* 11-04(primary), 11G20, 14G05(secondary).

This work was supported by JST PRESTO program.

absolutely irreducible over k, and the genus of the curve C defined by the equation

$$y^a = x^b(1-x^c)^d \tag{2.1}$$

is given by

$$g = \frac{1}{2}(ca - c\gcd(a,d) - \gcd(a,b) - \gcd(a,b+cd)) + 1.$$

Proof. From Proposition 1.1 and 1.3 in [**5**], we have the assertion. □

We remark that the curve 6.4 in [**2**] is similar to the case of $c|b$ of the curve defined by the equation of 2.1, and Lemma can also be proved by Proposition 3.7.10 in [**9**].

Let $k := \mathbb{F}_q$. It is possible to obtain curves with many rational points only when a divides $q-1$. Hence we use the algorithm in [**5**] to count the number of rational points of the curves defined by the equation 2.1 for a, b, c, d satisfying $a|(q-1)$, $b+cd < a$ and the condition in Lemma.

Since the defining equation is simple, it is suitable for computer search and also convinient for applications. After practicle search, we can find new curves with many rational points, which improve upon the lower bounds of 'Tables with many points' in [**3**] for $p = 3, 5, 7, 11, 13, 17, 19, 43, 89$. We list the defining equations of curves, integers q, genera and new entries of [**3**]. The lower bound of any entry is the number of rational points of the curve over the finite field $\mathbb{F}_q$.

TABLE 1. *($p = 3$)*

curve	q	genus	new entry
$y^{22} = x^{11}(1-x)$	3^5	5	[364-397]
$y^{22} = x^6(1-x)$	3^5	10	[444-551]

TABLE 2. *($p = 5$)*

curve	q	genus	new entry
$y^{16} = x^{10}(1-x)$	5^4	7	[788-976]
$y^{52} = x^2(1-x^2)$	5^4	49	[2400-3076]
$y^{11} = x^4(1-x)$	5^5	5	[3501-3681]
$y^{22} = x^7(1-x)$	5^5	10	[3876-4236]
$y^{44} = x^4(1-x)$	5^5	20	[4626-5346]

TABLE 3. *($p = 7$)*

curve	q	genus	new entry
$y^{24} = x^4(1-x)$	7^2	10	[150-186]
$y^{19} = x^2(1-x)$	7^3	9	[554-675]
$y^{38} = x^6(1-x)$	7^3	18	[764-1010]
$y^{57} = x^6(1-x)$	7^3	27	[974-1343]
$y^{20} = x^9(1-x)$	7^4	5	[2632-2892]
$y^{30} = x^{14}(1-x)$	7^4	7	[2748-3088]
$y^{20} = x(1-x)$	7^4	9	[3024-3284]
$y^{30} = x^2(1-x)$	7^4	13	[3336-3676]
$y^{20} = x^2(1-x^2)$	7^4	17	[3808-4068]

TABLE 4. $(p = 11)$

curve	q	genus	new entry
$y^{24} = x^{16}(1-x)$	11^2	8	[250-298]
$y^{19} = x^3(1-x)$	11^3	9	[1656-1980]
$y^{35} = x^4(1-x)$	11^3	15	[1932-2412]
$y^{38} = x^7(1-x)$	11^3	18	[2130-2628]
$y^{16} = x^{14}(1-x)$	11^4	7	[15460-16336]

TABLE 5. $(p = 13)$

curve	q	genus	new entry
$y^8 = x^2(1-x^2)$	13^2	5	[232-300]
$y^{21} = x(1-x)$	13^2	10	[339-430]
$y^{28} = x^2(1-x^2)$	13^2	25	[624-820]
$y^{12} = x^6(1-x^2)$	13^3	7	[2504-2849]
$y^{36} = x^{18}(1-x)$	13^3	9	[2648-3035]
$y^{18} = x^2(1-x^2)$	13^3	16	[3102-3686]
$y^{20} = x^{10}(1-x)$	13^4	5	[30152-30252]
$y^{20} = x(1-x)$	13^4	9	[31504-31604]
$y^{20} = x^2(1-x^2)$	13^4	17	[34208-34308]

TABLE 6. $(p = 17)$

curve	q	genus	new entry
$y^8 = x^2(1-x^2)$	17^2	5	[376-460]
$y^{32} = x^{21}(1-x)$	17^2	15	[612-800]
$y^8 = x^4(1-x^2)$	17^3	5	[5000-5612]
$y^{16} = x^5(1-x)$	17^3	7	[5204-5892]
$y^{16} = x^{10}(1-x^2)$	17^3	13	[5768-6732]
$y^{20} = x^{10}(1-x)$	17^4	5	[85512-86412]
$y^{16} = x^6(1-x)$	17^4	7	[86644-87568]
$y^{40} = x^2(1-x)$	17^4	19	[91804-94504]
$y^{60} = x^{18}(1-x)$	17^4	27	[96428-99128]
$y^{20} = x^4(1-x^4)$	17^4	35	[101052-103752]

TABLE 7. $(p = 19)$

curve	q	genus	new entry
$y^{40} = x^7(1-x)$	19^2	16	[762-970]
$y^{60} = x^{11}(1-x)$	19^2	24	[1034-1274]
$y^{18} = x^3(1-x)$	19^3	7	[7312-8015]
$y^{27} = x^8(1-x)$	19^3	9	[8057-8345]
$y^{54} = x^{18}(1-x)$	19^3	18	[9254-9830]
$y^{18} = x^2(1-x^3)^3$	19^3	22	[8760-10490]
$y^{24} = x^7(1-x)$	19^4	8	[132922-136098]

TABLE 8. $(p = 43, 89)$

curve	q	genus	new entry
$y^{14} = x^9(1-x)$	43	6	[100-116]
$y^8 = x^4(1-x^2)$	89	5	[136-180]

Acknowledgements. I would like to thank Shinji Miura and Takayuki Oda for their discussion. I used the algbraic system KASH/KANT for the computer search, so I would like to thank the authors.

References

1. D. K. FADEEV, 'On the divisor class groups of some algebraic curves', *Sov. Math.*2(1)(1961)67–69.
2. A. GARCIA, H. STICHTENOTH and C. P. XING, 'On subfields of the Hermitian function field', *Comp. Math.*120(2000)137–170.
3. G. VAN DER GEER, E. HOWE, K. LAUTER and C. RITZENTHALER, 'Table of curves with many points'. URL http://www.manypoints.org
4. J. W. P. HIRSCHFELD, G. KORCHMAROS and F. TORRES, 'Algebraic Curves over a Finite Field', *Princeton Series in Applied Mathematics*, (Princeton Univ. Press, Princeton, NJ, 2008).
5. M. Q. KAWAKITA, 'Kummer curves and their fibre products with many rational points', *Appl. Algebra Engrg. Comm. Comput.*14(1)(2003)55–64.
6. M. Q. KAWAKITA, 'On quotient curves of the Fermat curve of degree twelve attaining the Serre bound', *Internat. J. Math.* 20(5)(2009)529–539.
7. N. KOBLITZ and D. ROHRLICH 'Simple factors in the Jacobian of a Fermat curve', *Can. J. Math.*30(6)(1978)1183–1205.
8. H. NIEDERREITER and C. XING, 'Algebraic geometry in coding theory and cryptography', (Princeton Univ. Press, Princeton, NJ, 2009).
9. H. STICHTENOTH, 'Algebraic Function Fields and Codes', Second edition, *Graduate Texts in Math.*254, (Springer-Verlag, Berlin, 2009).

Motoko Qiu Kawakita
Division of Mathematics
Shiga University of Medical Science
Seta Tsukinowa-cho, Otsu, Shiga 520-2192
Japan

kawakita@belle.shiga-med.ac.jp